On the number of pairs of positive integers
x, $y \leq H$ such that $x^2 + y^2 + 1$ is squarefree

D. I. Tolev

Abstract   It is not difficult to find an asymptotic formula for the number of pairs of positive integers x, $y \leq H$ such that $x^2 + y^2 + 1$ is squarefree. In the present paper we improve the estimate for the error term in this formula using the properties of certain exponential sums. A.Weils's estimate for the Kloosterman sum plays the major role in our analysis.

Keywords   Squarefree numbers · Kloosterman sums

Mathematics Subject Classification (2000)   11L05 · 11N25 · 11N37

1 Notations

Let H be a sufficiently large positive number. By the letters k, m, n we denote integers and by d, r, l, h, q, x, y—positive integers. The letters t and D denote real numbers and the letter p is reserved for primes. By ε we denote an arbitrary small positive number, not necessarily the same in different occurrences. This convention allows us to write $q^\varepsilon \log q \ll q^\varepsilon$, for example. If it is not explicitly stated the opposite, the constants in the Vinogradov and Landau symbols are absolute or depend on ε.

We denote by $\mu(n)$ the Möbius function and by $\tau(n)$ the number of positive divisors of n. We write $(n_1, \ldots, n_k)$ for the greatest common divisor of $n_1, \ldots, n_k$. As usual $[t]$ and $\{t\}$ denote the integer part, respectively, the fractional part of t. We put

D. I. Tolev (✉)
Faculty of Mathematics and Informatics, Sofia University "St. Kl. Ohridsky",
5 J.Bourchier, 1164 Sofia, Bulgaria
e-mail: dtolev@fmi.uni-sofia.bg

$\rho(t) = \frac{1}{2} - \{t\}$ and let $||t||$ be the distance from t to the nearest integer. Further $e(t) = \exp(2\pi it)$ and $e_q(t) = e(t/q)$. For any q and k such that $(q, k) = 1$ we denote by $\overline{(k)}_q$ the inverse of k modulo q. If the value of the modulus is clear form the context then we write for simplicity $\overline{k}$. For any odd q we denote by $\left(\frac{\cdot}{q}\right)$ the Jacobi symbol. By $\square$ we mark an end of a proof or its absence.

In this paper we use the properties of the Gauss sum and the Kloosterman sum. They are defined by

$$G(q; n, m) = \sum_{1 \leq x \leq q} e_q\left(nx^2 + mx\right), \quad G(q; n) = G(q; n, 0) \tag{1}$$

and, respectively, by

$$K(q; n, m) = \sum_{\substack{1 \leq x \leq q \\ (x, q) = 1}} e_q(nx + m\overline{x}). \tag{2}$$

2 Introduction and statement of the result

Suppose that $f(t_1, \ldots, t_r)$ is a polynomial with integer coefficients and denote by $S_f(H)$ the number of r-tuples of positive integers $n_1, \ldots, n_r \leq H$ such that $f(n_1, \ldots, n_r)$ is squarefree. The problem is to evaluate $S_f(H)$ when H is large. A lot of articles are devoted to problems of this type. We point out the papers of Estermann [1], Filaseta [3], Greaves [4], Heath-Brown [5], Hooley [7,8], (see also the book [6], Chapter 4) and Poonen [11], but many other similar results can be found in literature.

In certain cases one can obtain an asymptotic formula for $S_f(H)$. For example Estermann [1] proved that

$$\sum_{1 \leq x \leq H} \mu^2\left(x^2 + 1\right) = c_0 H + O\left(H^{\frac{2}{3} + \varepsilon}\right),$$

where $c_0 > 0$ is a constant. We should mention that using his "square sieve" Heath-Brown's [5] considered $S_f(H)$ for the polynomial $f(t) = t(t+1)$ and found an asymptotic formula with error term $O\left(H^{\frac{7}{11} + \varepsilon}\right)$.

In the present paper we consider $S_f(H)$ for the polynomial $f(t_1, t_2) = t_1^2 + t_2^2 + 1$. We write for simplicity

$$S(H) = \sum_{1 \leq x, y \leq H} \mu^2(x^2 + y^2 + 1)$$

and denote

$$\lambda(q; n, m) = \sum_{x, y: (4)} e_q(nx + my), \tag{3}$$

where the summation is taken over the integers x, y satisfying the conditions

$$1 \leq x, y \leq q, \quad x^2 + y^2 + 1 \equiv 0 \pmod{q}. \tag{4}$$

We denote also

$$\lambda(q) = \lambda(q; 0, 0). \tag{5}$$

Our result is the following

Theorem *For the sum $S(H)$ we have*

$$S(H) = cH^2 + O\left(H^{\frac{4}{3}+\varepsilon}\right), \tag{6}$$

where

$$c = \prod_p \left(1 - \frac{\lambda\left(p^2\right)}{p^4}\right). \tag{7}$$

We note that if we apply simplest elementary methods only then we will find an asymptotic formula for $S(H)$ with an error term $O\left(H^{\frac{3}{2}+\varepsilon}\right)$. Our better result is a consequence of the estimate for $\lambda(q; n, m)$ established in Lemma 3, which can be obtained using the properties of the Gauss sum and A.Weil's estimate for the Kloosterman sum.

We may apply the same method for studying $S_f(H)$ with any quadratic polynomial f in two variables. (Of course trivial cases like $f(t_1, t_2) = (t_1 + t_2)^2$ have to be excluded.) Then the exponential sum

$$\lambda_f(q; n, m) = \sum_{\substack{1 \leq x, y \leq q \\ f(x,y) \equiv 0 \pmod{q}}} e_q(nx + my) \tag{8}$$

naturally appears. It is closely connected with the Kloosterman sum (and in the case $f(t_1, t_2) = t_1 t_2 - 1$ the sum (8) coincides with the Kloosterman sum), therefore we may use again A.Weil's estimate in order to estimate (8). However we shall not consider this more general problem here.

3 Lemmas

Our first lemma includes the basic properties of the Gauss sum. The proofs are available in Sect. 6 of [2] and Chapter 7 of [9].

Lemma 1 *For the Gauss sum we have*

(i) If $(q, n) = d$ then

$$G(q; n, m) = \begin{cases} d\, G(q/d; n/d, m/d) & \text{if } d \mid m, \\ 0 & \text{if } d \nmid m. \end{cases}$$

(ii)   *If* $(q, 2n) = 1$ *then*

$$G(q; n, m) = e_q\left(-\overline{(4n)}\, m^2\right)\left(\frac{n}{q}\right) G(q; 1).$$

(iii)   *If* $(q, 2) = 1$ *then*

$$G^2(q; 1) = (-1)^{\frac{q-1}{2}}\, q.$$

In the next lemma we present A. Weil's estimate for the Kloosterman sum. For the proof we refer the reader to Chapter 11 of [10].

Lemma 2 *We have*

$$|K(q; n, m)| \le \tau(q)\, q^{\frac{1}{2}}\, (q, n, m)^{\frac{1}{2}}.$$

Next we establish the following

Lemma 3 *If* $8 \nmid q$ *then*

$$|\lambda(q; n, m)| \le 16\, \tau^2(q)\, q^{\frac{1}{2}}\, (q, n, m)^{\frac{1}{2}}. \tag{9}$$

In particular we have

$$\lambda(q) \ll q^{1+\varepsilon}. \tag{10}$$

Remark 1 An estimate of type (9) holds for any positive integer q. We impose the condition $8 \nmid q$ because in this case the proof is slightly simpler and because in our analysis only such q appear.

Proof First we consider the case $2 \nmid q$. It is clear that from (1), (3) and (4) it follows

$$\begin{aligned}
\lambda(q; n, m) &= \sum_{1 \le x, y \le q} e_q(nx + my)\, q^{-1} \sum_{1 \le h \le q} e_q(h(x^2 + y^2 + 1)) \\
&= q^{-1} \sum_{1 \le h \le q} e_q(h)\, G(q; h, n)\, G(q; h, m). \\
&= q^{-1} \sum_{l \mid q} \sum_{\substack{1 \le h \le q \\ (h, q) = \frac{q}{l}}} e_q(h)\, G(q; h, n)\, G(q; h, m).
\end{aligned}$$

Now we apply Lemma 1, our assumption $2 \nmid q$ and the definition (2). We get

$$
\begin{aligned}
\lambda(q; n, m) &= q \sum_{\substack{l \mid q \\ \frac{q}{l} \mid (m,n)}} l^{-2} \sum_{\substack{1 \le r \le l \\ (r,l)=1}} e_l(r) \, G\left(l; r, nlq^{-1}\right) G\left(l; r, mlq^{-1}\right) \\
&= q \sum_{\substack{l \mid q \\ \frac{q}{l} \mid (m,n)}} l^{-2} \, G^2(l, 1) \sum_{\substack{1 \le r \le l \\ (r,l)=1}} e_l\left(r - \overline{(4r)}(n^2 + m^2)l^2 q^{-2}\right) \\
&= q \sum_{\substack{l \mid q \\ \frac{q}{l} \mid (m,n)}} (-1)^{\frac{l-1}{2}} \, l^{-1} \, K\left(l; 1, \overline{4}(n^2 + m^2)l^2 q^{-2}\right).
\end{aligned}
$$

From the last formula and Lemma 2 we find that if $2 \nmid q$ then

$$
|\lambda(q; n, m)| \le q \sum_{\substack{l \mid q \\ \frac{q}{l} \mid (m,n)}} \tau(l) \, l^{-\frac{1}{2}} \le q \, \tau(q) \sum_{r \mid (q,n,m)} q^{-\frac{1}{2}} \, r^{\frac{1}{2}} \le \tau^2(q) \, q^{\frac{1}{2}} (q, n, m)^{\frac{1}{2}}.
$$

$$(11)$$

Next we note that the function $\lambda(q; n, m)$ possesses a multiplicative property. More precisely, one can establish that if $(q_1, q_2) = 1$ then

$$
\lambda(q_1 q_2; n, m) = \lambda\left(q_1; n\overline{(q_2)}_{q_1}, m\overline{(q_2)}_{q_1}\right) \lambda\left(q_2; n\overline{(q_1)}_{q_2}, m\overline{(q_1)}_{q_2}\right). \qquad (12)
$$

(The proof is elementary and we leave it to the reader.) Now, in the general case, we represent $q = 2^h q_1$, where $2 \nmid q_1$ and $h \le 2$. We apply (11), (12) and the trivial estimate $|\lambda(2^h; n, m)| \le 2^{2h}$ and obtain (9).

Finally, it is clear that (10) follows directly from (9). $\qquad \square$

Lemma 4 *Suppose that $8 \nmid q$ and $D \ge 2$. Then for the sums*

$$
U = \sum_{1 \le n \le D} \frac{|\lambda(q; n, 0)|}{n}, \qquad V = \sum_{1 \le n, m \le D} \frac{|\lambda(q; n, m)|}{n \, m}.
$$

we have

$$
U \ll q^{\frac{1}{2} + \varepsilon} D^{\varepsilon}, \quad V \ll q^{\frac{1}{2} + \varepsilon} D^{\varepsilon}. \qquad (13)
$$

Proof From Lemma 3 it follows that

$$
U \ll q^{\frac{1}{2} + \varepsilon} \sum_{1 \le n \le D} \frac{(q, n)^{\frac{1}{2}}}{n} = q^{\frac{1}{2} + \varepsilon} \Sigma_0,
$$

say. Obviously

$$\Sigma_0 \ll \sum_{r|q} r^{\frac{1}{2}} \sum_{\substack{n \leq D \\ n \equiv 0 \pmod{r}}} \frac{1}{n} \ll \sum_{r|q} r^{-\frac{1}{2}} \log D \ll (qD)^\varepsilon \tag{14}$$

and the first inequality in (13) follows. To prove the second one we apply again Lemma 3 and use (14) to get

$$V \ll q^{\frac{1}{2}+\varepsilon} \sum_{1 \leq n,m \leq D} \frac{(q,n,m)^{\frac{1}{2}}}{n\,m} \ll q^{\frac{1}{2}+\varepsilon} \sum_{1 \leq n,m \leq D} \frac{(q,n)^{\frac{1}{2}}(q,m)^{\frac{1}{2}}}{n\,m} = q^{\frac{1}{2}+\varepsilon}\,\Sigma_0^2 \ll q^{\frac{1}{2}+\varepsilon}\,D^\varepsilon.$$

$\square$

Lemma 5 *For any $D \geq 2$ we have*

$$\rho(t) = \sum_{1 \leq |n| \leq D} \frac{e(nt)}{2\pi i n} + O\left(g(D,t)\right), \tag{15}$$

where $g(D,t)$ is a positive, infinitely many times differentiable and periodic with period one function of t. It can be represented as a Fourier series

$$g(D,t) = \sum_{n \in \mathbb{Z}} c_D(n)\,e(nt),$$

with coefficients $c_D(n)$ satisfying

$$c_D(n) \ll \frac{\log D}{D} \quad \text{for all} \quad n,$$

and

$$\sum_{|n| > D^{1+\varepsilon}} |c_D(n)| \ll D^{-A}.$$

Here $A > 0$ is arbitrarily large and the constant in the $\ll$–symbol depends on A and ε.

Proof It is well-known that $\rho(t)$ can be represented in a form similar to (15), but with a different form of the error term—with the function $\min\left(1, (D||t||)^{-1}\right)$ rather than $g(D,t)$. (For a proof we refer the reader to Chapter 2 of [6].) The proof of the present formula for $\rho(t)$ is available in [12]. $\square$

4 Proof of the theorem

We use the well-known identity $\mu^2(n) = \sum_{d^2|n} \mu(d)$ to write

$$S(H) = \sum_{1 \leq d \leq \sqrt{2H^2+1}} \mu(d) T\left(H, d^2\right),$$

where $T(H, q)$ is the number of pairs of positive integers $x, y \leq H$ satisfying the congruence $x^2 + y^2 + 1 \equiv 0 \pmod{q}$. We choose a parameter z satisfying

$$\sqrt{H} \leq z \leq H \tag{16}$$

and denote by S' the contribution to $S(H)$ coming from the terms with $z < d \leq \sqrt{2H^2+1}$. It is clear that

$$T\left(H, d^2\right) = \sum_{1 \leq l \leq (2H^2+1)\, d^{-2}} \sum_{\substack{1 \leq x, y \leq H \\ x^2+y^2=ld^2-1}} 1 \ll H^{2+\varepsilon} d^{-2}.$$

Hence we obtain $S' \ll H^{2+\varepsilon} z^{-1}$ and therefore

$$S(H) = \sum_{1 \leq d \leq z} \mu(d) T\left(H, d^2\right) + O\left(H^{2+\varepsilon} z^{-1}\right). \tag{17}$$

From this point onwards we assume that $q = d^2$, where d is squarefree and $d \leq z$. Denote by $M(H, q, x)$ the number of positive integers $h \leq H$ satisfying $h \equiv x \pmod{q}$. Obviously

$$M(H, q, x) = H q^{-1} + O(1). \tag{18}$$

It is clear that

$$T(H, q) = \sum_{x, y:\, (4)} M(H, q, x) M(H, q, y). \tag{19}$$

If we use (17)–(19) and choose $z = \sqrt{H}$ then we may find an asymptotic formula for $S(H)$ with an error term $O(H^{\frac{3}{2}+\varepsilon})$. To establish our sharper result we represent the error term in (18) in an explicit form. First we write

$$M(H, q, y) = \left[\frac{H-y}{q}\right] - \left[\frac{-y}{q}\right] = \frac{H}{q} + \rho\left(\frac{H-y}{q}\right) - \rho\left(\frac{-y}{q}\right). \tag{20}$$

We substitute the last expression for $M(H, q, y)$ in (19) and denote by T' the contribution to $T(H, q)$ coming from the last term in the right-hand side of (20). Next we

represent T' as

$$T' = T'' + T''', \tag{21}$$

where T'' consists of the terms for which $x^2 + 1 \equiv 0 \pmod{q}$ and T''' is the contribution of the other terms. We have

$$T''' = - \sum_{\substack{1 \le x \le q \\ x^2+1 \not\equiv 0 \ (\mathrm{mod}\ q)}} M(H,q,x) \sum_{\substack{1 \le y \le q \\ y^2 \equiv -x^2-1 \ (\mathrm{mod}\ q)}} \rho\left(\frac{-y}{q}\right) = 0 \tag{22}$$

because the last sum over y vanishes. Indeed, it does not contain terms with $y = \frac{q}{2}$ and $y = q$. Further, for any y satisfying the congruence condition and such that $1 \le y < \frac{q}{2}$ the integer $q - y$ satisfies the same congruence and we have $\rho\left(\frac{-y}{q}\right) + \rho\left(\frac{-(q-y)}{q}\right) = 0$.

Consider now T''. We have

$$T'' = - \sum_{\substack{1 \le x \le q \\ x^2+1 \equiv 0 \ (\mathrm{mod}\ q)}} M(H,q,x) \sum_{\substack{1 \le y \le q \\ y^2 \equiv 0 \ (\mathrm{mod}\ q)}} \rho\left(\frac{-y}{q}\right) \ll H^\varepsilon \left(Hq^{-1} + 1\right).$$

$$\tag{23}$$

Indeed, the last sum over y equals $O(1)$ because, according to the above arguments, it reduces to a sum with at most two terms (corresponding to $y = \frac{q}{2}$ and $y = q$). Further, the number of solutions of the congruence $x^2 + 1 \equiv 0 \pmod{q}$ equals $O(q^\varepsilon)$ and applying (18) we obtain (23).

From (21)–(23) we get $T' \ll H^\varepsilon \left(Hq^{-1} + 1\right)$ and therefore

$$T(H,q) = \sum_{x,y:(4)} M(H,q,x) \left(\frac{H}{q} + \rho\left(\frac{H-y}{q}\right)\right) + O\left(H^\varepsilon \left(Hq^{-1} + 1\right)\right).$$

We proceed with the quantity $M(H,q,x)$ in a similar manner and we conclude that

$$T(H,q) = \sum_{x,y:(4)} \left(\frac{H}{q} + \rho\left(\frac{H-x}{q}\right)\right) \left(\frac{H}{q} + \rho\left(\frac{H-y}{q}\right)\right) + O\left(H^\varepsilon \left(Hq^{-1} + 1\right)\right).$$

Now we use (3) and (5) to find

$$T(H,q) = \frac{H^2 \lambda(q)}{q^2} + 2\frac{H}{q} T_1(H,q) + T_2(H,q) + O\left(H^\varepsilon \left(Hq^{-1} + 1\right)\right), \tag{24}$$

where

$$T_1(H, q) = \sum_{x, y: (4)} \rho\left(\frac{H - x}{q}\right), \tag{25}$$

$$T_2(H, q) = \sum_{x, y: (4)} \rho\left(\frac{H - x}{q}\right) \rho\left(\frac{H - y}{q}\right). \tag{26}$$

Consider $T_1(H, q)$. We apply (3) and Lemma 5 with $D = H$ to get

$$T_1(H, q) = T_1'(H, q) + O\left(T_1^*(H, q)\right), \tag{27}$$

where

$$T_1'(H, q) = \sum_{x, y: (4)} \sum_{1 \le |n| \le H} \frac{e_q(n(H - x))}{2\pi i n} = \sum_{1 \le |n| \le H} \frac{e_q(nH)\lambda(q; -n, 0)}{2\pi i n},$$

$$T_1^*(H, q) = \sum_{x, y: (4)} g\left(H, \frac{H - x}{q}\right). \tag{28}$$

From Lemma 4 it follows that

$$T_1'(H, q) \ll H^\varepsilon q^{\frac{1}{2}}. \tag{29}$$

To estimate $T_1^*(H, q)$ we apply (3) and Lemmas 3, 4 and 5 and obtain

$$T_1^*(H, q) = \sum_{x, y: (4)} \left(c_H(0) + \sum_{1 \le |n| \le H^{1+\varepsilon}} c_H(n)\, e_q(n(H - x))\right) + O(1)$$

$$= c_H(0)\lambda(q) + \sum_{1 \le |n| \le H^{1+\varepsilon}} c_H(n)\, e_q(nH)\, \lambda(q; -n, 0) + O(1)$$

$$\ll H^{\varepsilon-1} q + 1 + H^{\varepsilon-1} \sum_{1 \le |n| \le H^{1+\varepsilon}} |\lambda(q; -n, 0)|$$

$$\ll H^{\varepsilon-1} q + 1 + H^\varepsilon \sum_{1 \le n \le H^{1+\varepsilon}} \frac{|\lambda(q; n, 0)|}{n}$$

$$\ll H^{\varepsilon-1} q + H^\varepsilon q^{\frac{1}{2}}. \tag{30}$$

From (27), (29) and (30) we get

$$T_1(H, q) \ll H^{\varepsilon-1} q + H^\varepsilon q^{\frac{1}{2}}. \tag{31}$$

Consider now $T_2(H, q)$. We apply (26), (28), (30) and Lemmas 4 and 5, to get

$$T_2(H, q) = \sum_{x, y:\,(4)} \sum_{1 \leq |n|, |m| \leq H} \frac{e_q\left((n + m)H\right) e_q\left(-nx - my\right)}{(2\pi i)^2 nm} + O\left(H^\varepsilon T_1^*(H, q)\right)$$

$$= \sum_{1 \leq |n|, |m| \leq H} \frac{e_q\left((n + m)H\right)}{(2\pi i)^2 nm} \lambda(q; -n, -m) + O\left(H^{\varepsilon-1} q + H^\varepsilon q^{\frac{1}{2}}\right)$$

$$\ll \sum_{1 \leq |n|, |m| \leq H} \frac{|\lambda(q; n, m)|}{|nm|} + H^{\varepsilon-1} q + H^\varepsilon q^{\frac{1}{2}}$$

$$\ll H^{\varepsilon-1} q + H^\varepsilon q^{\frac{1}{2}}. \tag{32}$$

From (24), (31) and (32) it follows that

$$T(H, q) = H^2 \frac{\lambda(q)}{q^2} + O\left(H^\varepsilon (H q^{-\frac{1}{2}} + q^{\frac{1}{2}} + H^{-1} q)\right).$$

We use the above formula, (16) and (17) and we get

$$S(H) = H^2 \sum_{1 \leq d \leq z} \frac{\mu(d)\lambda\left(d^2\right)}{d^4} + O\left(H^\varepsilon \left(H + z^2 + H^{-1} z^3 + H^2 z^{-1}\right)\right)$$

$$= c\, H^2 + O\left(H^\varepsilon \left(H^2 z^{-1} + z^2\right)\right),$$

where $c = \sum\limits_{d=1}^{\infty} \frac{\mu(d)\lambda(d^2)}{d^4}$. (Clearly this number coincides with the product at (7)). It remains to choose $z = H^{\frac{2}{3}}$ and the proof of the theorem is complete.

References

1. Estermann, T.: Einige Sätze über quadratfreie Zahlen. Math. Ann. **105**, 653–662 (1931)
2. Estermann, T.: A new application of the Hardy–Littlewood–Kloosterman method. Proc. Lond. Math. Soc., **12**, 425–444 (1962)
3. Filaseta, M.: Powerfree values of binary forms. J. Number Theory **49**(2), 250–268 (1994)
4. Greaves, G.: Power-free values of binary forms. Q. J. Math. **43**, 45–65 (1992)
5. Heath-Brown, D.R.: The square sieve and consecutive square-free numbers. Math. Ann. **266**, 251–259 (1984)
6. Hooley, C.: Applications of sieve methods to the theory of numbers. Cambridge University Press, Cambridge (1976)
7. Hooley, C.: On the power-free values of polynomials in two variables, Roth 80th birthday volume (in press)
8. Hooley, C.: On the power-free values of polynomials in two variables: II. J. Number Theory **129**, 1443–1455 (2009)
9. Hua, L.-K.: Introduction to number theory. Springer, Berlin (1982)

10. Iwaniec, H., Kowalski, E.: Analytic number theory. Colloquium Publications, vol. 53, Am. Math. Soc., (2004)
11. Poonen, B.: Squarefree values of multivariable polynomials. Duke Math. J. **118**(2), 353–373 (2003)
12. Tolev, D.: On the exponential sum with squarefree numbers. Bull. Lond. Math. Soc. **37**(6), 827–834 (2005)